SENAFTI
SEMINAR NASIONAL MAHASISWA FAKULTAS TEKNOLOGI INFORMASI

5th Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)
7 September 2024 – Jakarta, Indonesia
Volume 3, Nomor 2, September 2024 - ISSN 2962-8628 (*online*)

PENGAMANAN PENGIRIMAN FILE MENGGUNAKAN STEGANOGRAFI DENGAN METODE LSB DI PT CAPTURE IT

Jonathan Tinambunan[1*], Sri Mulyati[2]

[1,2] Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur, Jakarta, Indonesia

Email: [1*]2011510985@student.budiluhur.ac.id, [2]sri.mulyati@budiluhur.ac.id
(* : corresponding author)

Abstrak- PT Capture It adalah penyedia layanan *photobooth* dan *videobooth* terkemuka di Indonesia yang telah melayani berbagai momen istimewa selama lebih dari 12 tahun. Dengan pengalaman dan inovasi yang ditawarkan, PT Capture It menjadi pilihan utama dalam memberikan layanan yang mengabadikan momen berharga secara visual. Dalam era digital yang semakin berkembang, pengamanan data menjadi isu yang penting, khususnya dalam industri fotografi dan penyimpanan file digital. Penelitian ini bertujuan untuk mengembangkan aplikasi steganografi menggunakan teknik *Least Significant Bit* (LSB) untuk mengamankan data digital di PT Capture It. Beberapa pertanyaan yang diangkat dalam penelitian ini meliputi bagaimana penerapan teknik LSB dalam mengamankan data, dampaknya terhadap kualitas gambar, serta efektivitasnya dalam melindungi hak cipta melalui watermark. Selain itu, penelitian ini juga mengevaluasi ketahanan metode steganografi tersebut terhadap serangan seperti *blur*, kompresi JPEG, dan *noise salt and pepper*. Metode yang digunakan dalam penelitian ini melibatkan pengembangan aplikasi steganografi yang mampu menyematkan informasi unik atau hak cipta ke dalam foto digital tanpa mempengaruhi kualitas visual gambar. Aplikasi ini kemudian diuji dengan mengunggah gambar ke *google drive* untuk mengevaluasi apakah data yang disisipkan tetap dapat diekstraksi setelah melalui proses pengunggahan. Penilaian terhadap hasil steganografi dilakukan menggunakan metrik PSNR, MSE, dan CC, yang memberikan gambaran tentang kualitas dan integritas gambar setelah disisipkan data. Hasil penelitian menunjukkan bahwa teknik LSB dapat secara efektif digunakan untuk menyematkan informasi ke dalam gambar digital dengan dampak minimal pada kualitas visual. Selain itu, data yang disisipkan terbukti tetap dapat diekstraksi dengan baik meskipun gambar telah melalui proses pengunggahan dan kompresi. Penelitian ini memberikan kontribusi penting dalam pengembangan metode pengamanan data digital di industri fotografi, khususnya di PT Capture It.

Kata Kunci: Steganografi, *Least Significant Bit* (LSB), *Mean Squared Error* (MSE), *Peak Signal-to-Noise Ratio* (PSNR), *Coefficient Correlation* (CC)

SECURING FILE DELIVERY USING STEGANOGRAPHY WITH LSB METHOD IN PT. CAPTURE IT

Abstract- *PT Capture It is a leading photobooth and videobooth service provider in Indonesia that has been serving various special moments for more than 12 years. With its experience and innovation, PT Capture It is the first choice in providing services that visually capture precious moments. In the growing digital era, data security has become an important issue, especially in the photography industry and digital file storage. This research aims to develop a steganography application using the Least Significant Bit (LSB) technique to secure digital data at PT Capture It. Some of the questions raised in this research include how the LSB technique is applied in securing data, its impact on image quality, and its effectiveness in protecting copyright through watermarks. In addition, this research also evaluates the robustness of the steganography method against attacks such as blur, JPEG compression, and salt and pepper noise. The method used in this research involves the development of a steganography application capable of embedding unique or copyright information into a digital photograph without affecting the visual quality of the image. The application is then tested by uploading the image to google drive to evaluate whether the inserted data can still be extracted after going through the upload process. Assessment of the steganography results is done using PSNR, MSE, and CC metrics, which give an idea of the quality and integrity of the image after the data is inserted. The results show that the LSB technique can be effectively used to embed information into digital images with minimal impact on visual quality. In addition, the inserted data was shown to still be extracted properly even though the image has gone through uploading and compression processes. This research makes an important contribution to the development of digital data security methods in the photography industry, especially at PT Capture It.*

Keywords*: Steganography, Least Significant Bit (LSB), Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), Coefficient Correlation (CC)*

1. PENDAHULUAN

Di era digital saat ini, keamanan data menjadi prioritas utama bagi berbagai organisasi, termasuk PT Capture It. Dengan meningkatnya volume data yang dipertukarkan secara digital, informasi sensitif menjadi target utama kejahatan siber, sehingga perlindungan data menjadi sangat penting untuk menjaga kerahasiaan dan integritas informasi.

PT Capture It adalah penyedia layanan *photobooth* dan *videobooth* terlengkap di Indonesia. Dengan pengalaman lebih dari 12 tahun, perusahaan ini telah menjadi pilihan utama untuk mengabadikan momen-momen berharga di berbagai acara, mulai dari pernikahan hingga acara perusahaan. PT Capture It dikenal dengan inovasi dan teknologi terkini, termasuk penggunaan Artificial Intelligence (AI) dalam layanan mereka. Mereka menawarkan berbagai jenis photobooth unik seperti Photobox Classic, Photobooth Hologram, 360 Videobooth, dan lainnya, yang semuanya dirancang untuk memberikan pengalaman yang tak terlupakan bagi para pengguna.

PT Capture It menghadapi tantangan dalam melindungi informasi sensitif dan hak cipta gambar yang mereka hasilkan. Insiden kebocoran informasi, seperti pencurian ide produk baru dan pencurian karya telah menimbulkan kerugian finansial dan merusak reputasi perusahaan. Selain itu, gambar-gambar yang digunakan dalam proyek dan kampanye pemasaran perusahaan perlu dilindungi dari penggunaan ilegal.

Untuk mengatasi masalah ini, steganografi dengan teknik *Least Significant Bit* (LSB) digunakan sebagai solusi untuk pengamanan pengiriman file. LSB merupakan algoritma sederhana namun dapat digunakan pada proses steganografi [1]. Penyembunyian pesan dengan menggunakan metode LSB sangat sederhana karena hanya mengubah nilai bit terakhir dengan bit pesan [2].

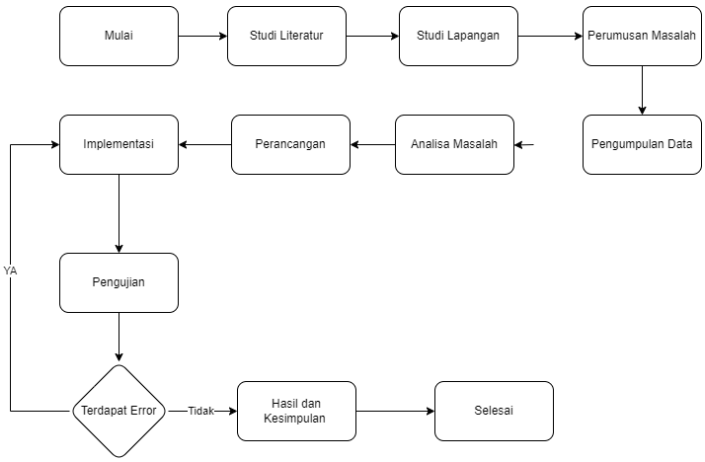
Pada Penelitian yang dilakukan oleh Cahaya Jatmoko, dll pada tahun 2018 mengevaluasi kinerja dua algoritma steganografi, *Least Significant Bit* (LSB) dan *Most Significant Bit* (MSB), dalam menyembunyikan pesan di dalam gambar digital untuk meningkatkan keamanan komunikasi. Penelitian ini membandingkan kualitas pesan yang disembunyikan dan ketahanannya terhadap berbagai serangan dengan menggunakan metrik seperti Mean Square Error (MSE) dan Peak Signal to Noise Ratio (PSNR). Temuan mengungkapkan bahwa LSB memberikan kualitas gambar yang lebih baik, sementara MSB menunjukkan ketahanan yang lebih besar terhadap serangan tertentu seperti *noise salt and pepper*. penelitian ini menyoroti perlunya analisis lebih lanjut dan peningkatan kedua algoritma tersebut dalam aplikasi steganografi [3].

Sri Winda dll. pada tahun 2019 menerapkan algoritama steganografi dengan metode *Least Significant Bit* (LSB) dan RC4 untuk melindungi informasi pasien yang sensitif di klinik Siti Rahmah, mendemonstrasikan metode yang efektif untuk menyematkan pesan terenkripsi di dalam gambar dan memastikan perlindungan data melalui kombinasi teknik kriptografi dan steganografi [4]. Perbedaan antara penelitian sebelumnya adalah penelitian ini hanya menggunakan metode LSB saja. penelitian ini terletak pada kemampuan untuk mengenkripsi dan mendekripsi gambar.

Berdasarkan latar belakang yang telah dijelaskan penulis membangun aplikasi steganografi dengan metode *Least Significant Bit* (LSB) untuk menyisipkan informasi penting untuk mengamankan data tersebut sehingga tidak disalahgunakan atau dicuri oleh pihak-pihak yang tidak bertanggung jawab. LSB sudah diuji dari beberapa penelitian sebelumnya bahwa dapat mengamankan file dengan sangat baik. Data yang sudah teresnkripsi hanya akan diakses oleh tim internal PT Capture It.

2. METODE PENELITIAN

Untuk memastikan bahwa hasil penelitian sesuai dengan tujuan yang telah ditetapkan, metode penelitian bertindak sebagai panduan dan acuan. Gambar 1 menguraikan langkah-langkah yang diambil untuk menerapkan metodologi penelitian yang digunakan dalam penelitian ini.



Gambar 1. Metode Penelitian

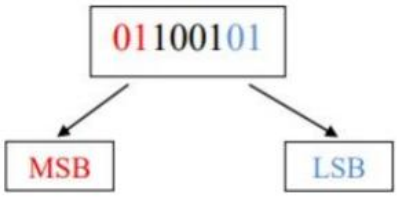
a. Tinjauan literatur, pengumpulan informasi, dan analisis dari berbagai sumber, termasuk buku, artikel jurnal, dan materi lainnya, diperlukan untuk memahami steganografi dan pendekatan LSB dan untuk membantu para peneliti membuat kesimpulan yang terinformasi dengan baik.
b. Studi Lapangan dengan PT Capture It diperlukan untuk mengumpulkan data dan memahami masalah yang dihadapi agar dapat mengimplementasikan solusi yang disarankan dengan benar.
c. Perumusan masalah, menetapkan masalah utama yaitu untuk mengamankan data dan memberikan watermark kedalam gambar dengan metode LSB.
d. Pengumpulan data dilakukan dengan cara wawancara .
e. Analisa masalah melalui banyak fase analisis diperlukan untuk penelitian ini. Di antara tahapan-tahapan tersebut meliputi analisa data, analisa penerapan algoritma, dan analisa sistem.
f. Perancangan, merancang sistem berdasarkan analisis yang telah dilakukan.
g. Implementasi, mengubah desain modul ke dalam Bahasa pemrograman python dengan perangkat keras Intel Core I5, RAM 24GB, dan SSD 512GB.
h. Hasil dan Kesimpulan, menarik kesimpulan tentang keampuhan penggunaan pendekatan LSB untuk mengamankan file dan menawarkan rekomendasi untuk meningkatkan dan memperluas sistem.

2.1 Data Penelitian

Data penelitian ini diambil dari PT Capture It, data yang dikumpulkan terdiri dari berbagai jenis gambar yang dihasilkan PT. Capture it. Proses pengambilan data dilakukan dengan cermat untuk memastikan akurasi dan kualitas data yang digunakan dalam analisis steganografi. Data tersebut kemudian dianalisis untuk menguji implementasi metode LSB dalam menyembunyikan informasi di dalam gambar.

2.2 Metode LSB

Salah satu teknik steganografi dalam ranah spasial, LSB, menyisipkan pesan dengan mengubah nilai bit terkecil. Dalam konteks ini, steganografi digital telah mendorong pengembangan aplikasi yang inovatif di dunia bisnis, memastikan bahwa bidang ini terus berkembang. Sebagai contoh, penelitian terbaru oleh Antonius dll (2018) mengeksplorasi teknik yang memanfaatkan empat bit paling tidak signifikan (LSB) untuk menyisipkan dan menguraikan data secara efisien [5].



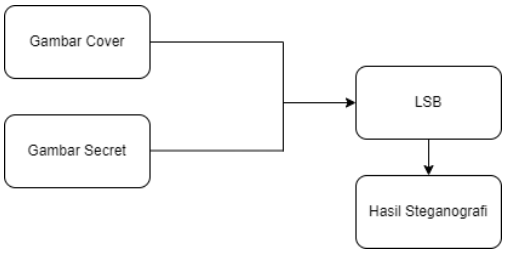
Gambar 2. Perbedaan MSB dan LSB

Teknik steganografi LSB memanfaatkan fakta bahwa perubahan kecil pada bit terakhir piksel gambar (Lihat Gambar 2) tidak secara signifikan mempengaruhi penampilan visual gambar tersebut [6]. Dengan memodifikasi

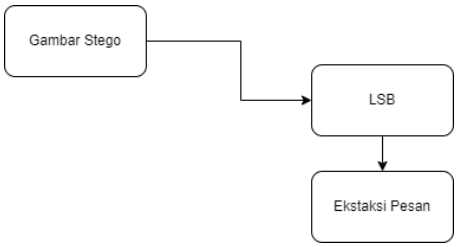
bit-bit ini, sebuah gambar bisa ditambahkan pesan rahasia ke dalamnya tanpa mengubah tampilan luarnya secara drastis. Untuk menilai kemiripan hasil gambar steganografi.

2.3 Analisa dan Perancangan

Berdasarkan data yang telah didapatkan maka dalam penelitian ini dirancang dua proses utama, yaitu proses penyisipan pesan metode LSB dan proses dekripsi pesan metode LSB. Gambar 3 merupakan proses penyisipan pesan dan Gambar 4 merupakan proses dekrispsi pesan



Gambar 3. Proses Penyisipan Pesan



Gambar 4. Proses Ekstraksi Pesan

2.4 Evaluasi Hasil dan Pengukuran

Dua langkah pengukuran dilakukan dalam penelitian ini: satu pada gambar stego dan satu lagi pada gambar pesan yang diekstrak. PSNR dan MSE digunakan untuk mengukur gambar stego. Perbandingan gambar cover dengan gambar stego menghasilkan nilai MSE dan PSNR. Dalam mengukur kualitas gambar, penaksir yang paling populer adalah *Mean Square Error* (MSE). Angka yang mendekati nol mengindikasikan performa yang unggul, karena ini adalah metrik referensi yang lengkap [7]. Sedangkan *Peak Signal-to-Noise Ratio* (PSNR) adalah kekuatan sinyal maksimum yang dapat dicapai terhadap derau yang kuat, yang menurunkan kualitas representasi. PSNR sering dinyatakan dalam skala desibel. PSNR adalah probabilitas bahwa beberapa rekonstruksi yang baik yang dibuat oleh manusia [8]. MSE dan PSNR sering digunakan untuk mengukur kualitas hasil steganografi dalam gambar, di mana nilai PSNR yang lebih tinggi menunjukkan kualitas gambar yang lebih baik. Semakin tinggi nilai PSNR maka semakin menyerupai gambar asli, sebaliknya jika gambar asli semakin tidak menyerupai aslinya, semakin tinggi MSE-nya [9]. Rumus MSE dan PSNR dapat dilihat pada persamaan (1).

$$MSE = \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} \|c(m,n) - s(m,n)\|^2 \quad (1)$$

$$PSNR_{dB} = 10\, log_{10} \left(\frac{255^2}{MSE} \right) \quad (2)$$

Keterangan:
a. m dan n adalah ukuran gambar
b. c merupakan gambar cover
c. s adalah gambar yang sudah di proses.

Saat gambar hasil ekstraksi diukur, alat ukur *correlation coefficient* (CC) digunakan. Dengan membandingkan gambar pesan yang diambil dengan gambar pesan asli, nilai CC dapat ditentukan [10]. CC

dihitung dengan menggunakan persamaan. Semakin mendekati angka 1 maka hasil akan semakin serupa dengan gambar asli. Berikut adalah rumus (2).

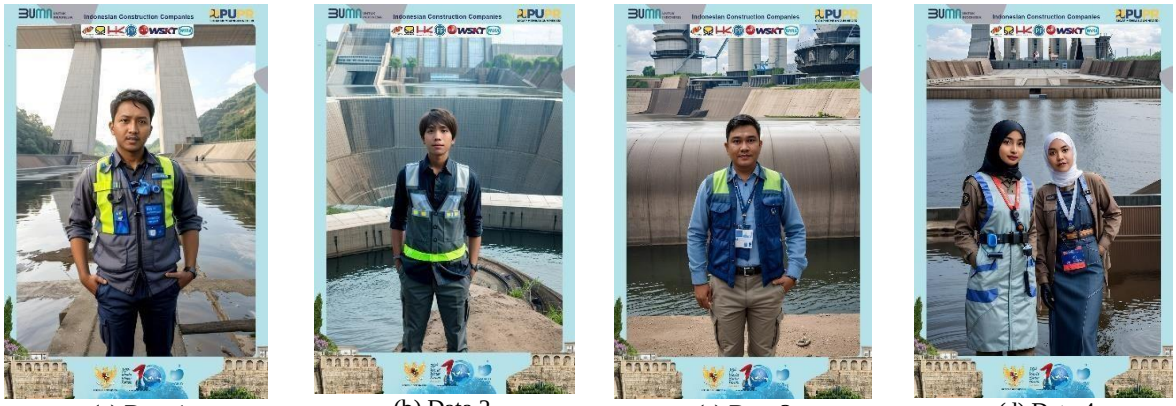
$$CC = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n}[p(i,j).e(i,j)]}{\sum_{i=1}^{m}\sum_{j=1}^{n}(p(i,j))^2} \quad (2)$$

Dimana:
a. m dan n adalah ukuran gambar
b. p merupakan gambar pesan asli
c. e adalah gambar pesan hasil ekstraksi

3. HASIL DAN PEMBAHASAN

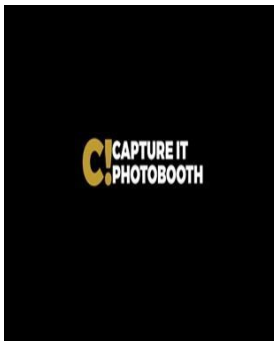
3.1 Penyisipan Pesan

Data diambil dari PT Capture it. Akan ada data *container* dan data *secret*. Gambar 5 adalah data yang gunakan sebagai gambar *container* dan Gambar 6 sebagai data yang akan disisipkan



(a) Data 1 (b) Data 2 (c) Data 3 (d) Data 4

Gambar 5. Gambar *Container*



Gambar 6. Gambar *Secret*

Gambar 5 merupakan merupakan data yang digunakan sebagai gambar *container*, sedangkan gambar 6 digunakan sebagai gambar *secret*. Data satu disisipkan menggunakan 1 *frame*, data 2 dengan 2 *frame*, data 3, dengan 3 *frame*, dan data 4 dengan 4 *frame*. Dimana semakin kecil *frame* yang disisipkan hasilnya akan semakin baik. Lihat Tabel 1.

Tabel 1. Nilai MSE dan PSNR penyisipan pesan

Gambar	MSE	PSNR
Data 1	0.52	50.96 dB
Data 2	3.28	42.97 dB
Data 3	16.58	35.94 dB
Data 4	70.89	29.63 dB

Data 1 Data 2 Data 3 Data 4

Gambar 7. Gambar Hasil Penyisipan

Keterangan Gambar :
a. Data 1 Disisipkan 1 *frame*
b. Data 2 Disisipkan 2 frame
c. Data 3 Disisipkan 3 frame
d. Data 4 Disisipkan 4 frame

Tabel 1 menunjukkan bahwa nilai MSE dan PSNR secara relatif sangat bagus. Apabila dilihat secara kasat mata, gambar yang sudah disisipkan seharusnya memiliki penampilan yang sama seperti gambar aslinya, karena nilai PSNR yang cukup bagus. Bisa dilihat semakin rendah LSB frame yang disisipkan Nilai dari PSNR semakin besar.

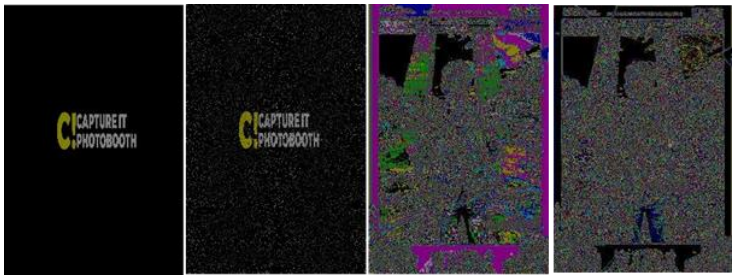
3.2 Ekstraksi Pesan

Ekstraksi pesan yang sempurna harus dapat dilakukan dengan teknik steganografi yang sesuai. Jika pesan tidak dapat sepenuhnya dipahami, pesan tersebut mungkin memiliki beberapa interpretasi berbeda. Nilai CC yang dihasilkan oleh pendekatan LSB ditampilkan pada Tabel 2 di bawah ini.

Tabel 2. Nilai CC Hasil Ekstraksi Pesan

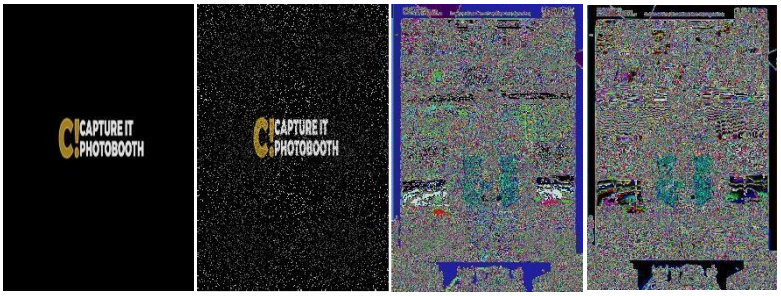
Gambar	Tanpa Serangan	Salt and Papper	JPEG	Blur
Data 1	1	0.4889	0.0184	0.0483
Data 2	1	0.4552	0.0315	0.0530
Data 3	1	0.4483	0.0450	0.0558
Data 4	1	0.4471	0.0480	0.0768

Tiga jenis serangan yang berbeda juga diperiksa dalam penelitian ini: blur, kompresi JPEG, dan salt & pepper. Terlihat jelas dari Gambar 8 dan Tabel 2 bahwa pendekatan LSB sangat rentan terhadap beberapa jenis serangan. Pesan hanya tahan terhadap serangan dengan salt & pepper.

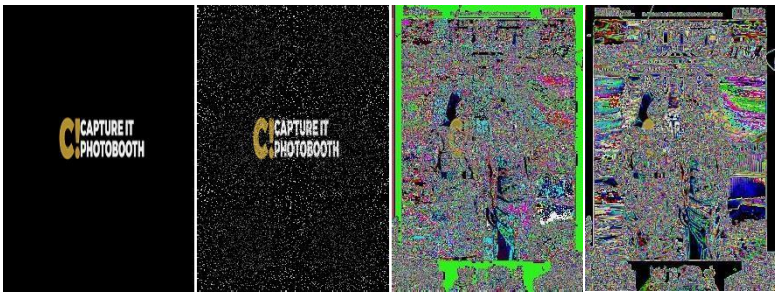


(a) Data 1

(b) Data 2



(c) Data 3



(d) Data 4

Gambar 8. Gambar Secret Hasil Ekstarksi

Keterangan Gambar:

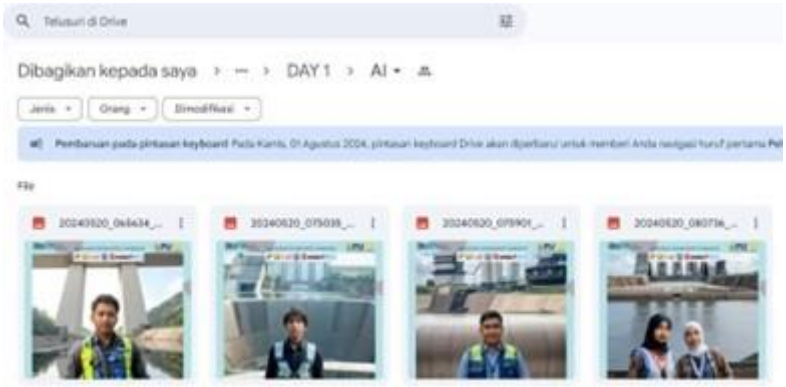
a. Hasil ekstarksi dari data 1 dengan LSB *Frame* 1 tanpa serangan
   Hasil ekstarksi dari data 1 dengan LSB *Frame* 1 dengan serangan *salt and papper*
   Hasil ekstarksi dari data 1 dengan LSB *Frame* 1 dengan serangan JPEG
   Hasil ekstarksi dari data 1 dengan LSB *Frame* 1 dengan serangan *blur*
b. Hasil ekstarksi dari data 2 dengan LSB *Frame* 2 tanpa serangan
   Hasil ekstarksi dari data 2 dengan LSB Frame 2 dengan serangan salt and papper
   Hasil ekstarksi dari data 2 dengan LSB Frame 2 dengan serangan JPEG
   Hasil ekstarksi dari data 2 dengan LSB *Frame* 2 dengan serangan *blur*
c. Hasil ekstarksi dari data 3 dengan LSB *Frame* 3 tanpa serangan
   Hasil ekstarksi dari data 3 dengan LSB Frame 3 dengan serangan salt and papper
   Hasil ekstarksi dari data 3 dengan LSB Frame 3 dengan serangan JPEG
   Hasil ekstarksi dari data 3 dengan LSB *Frame* 3 dengan serangan *blur*
d. Hasil ekstarksi dari data 4 dengan LSB *Frame* 4 tanpa serangan
   Hasil ekstarksi dari data 4 dengan LSB Frame 4 dengan serangan salt and papper
   Hasil ekstarksi dari data 4 dengan LSB Frame 4 dengan serangan blur
   Hasil ekstarksi dari data 4 dengan LSB *Frame* 4 dengan serangan *blur*

Tabel 2 mengilustrasikan bahwa jika tidak ada serangan, manipulasi, atau gangguan selama prosedur pengiriman gambar, gambar stego dari teknik LSB dapat diambil dengan sempurna. Tiga jenis kompresi *blur*, *salt*

& pepper, dan JPEG juga diselidiki dalam penelitian ini dimana, sudah dibuktikan bahwa metode LSB lemah terhadap ketiga serangan tersebut. Hanya serangan *salt & papper* saja yang mampu bertahan.

3.3 Pengujian *Google Drive*

Setelah gambar sudah di sisipkan, hasilnya akan diunggah ke *google drive* untuk memastikan apakah gambar yang sudah disisipkan pesan akan tetap utuh atau berubah. Hasil prosesnya dapat dilihat pada Gambar 9.



Gambar 9. Gambar Hasil Unggah Ke *Google Drive*

Setelah gambar sudah diunggah, dilakukan pengujian *decode* kembali untuk memastikan apakah gambar yang sudah disisipkan tetap utuh atau tidak. Hasil prosesnya dapat dilihat pada Gambar 10.

Gambar 10. Gambar Hasil Ekstraksi Setelah Di Unggah Ke *Google Drive*

Berdasarkan pengujian diatas, dapat disimpulkan bahwa gambar yang telah disisipkan tetap utuh setelah di upload ke *google drive*. Tabel 3 Menunjukan nilai PSNR, MSE Gambar yang sudah di upload ke *google drive*.

Tabel 3. Nilai MSE dan PSNR Setelah Unggah Ke *Google Drive*

Gambar	MSE	PSNR
Data 1	0.52	50.96 dB

Tabel 4 memperlihatkan hasil penilaian *Correlation Coefficient* (CC) pada gambar yang sudah di *upload* ke *google drive*.

Tabel 4. Nilai CC Setelah Unggah Ke *Google Drive*

Gambar	Tanpa Serangan	Salt and Papper	JPEG	Blur
Data 1	1	0.4889	0.0184	0.0483

4. KESIMPULAN

Penelitian ini mengevaluasi penggunaan steganografi metode LSB untuk mengamankan transmisi file di PT Capture It. Hasilnya menunjukkan bahwa metode LSB mampu menyisipkan pesan dalam gambar dengan minimal pengaruh pada kualitas visual, terbukti dengan nilai PSNR yang tinggi dan MSE yang rendah. Metode ini juga berhasil menyembunyikan informasi sensitif secara aman dan efisien, memungkinkan ekstraksi data dengan akurasi tinggi. Selain itu, metode LSB efektif melawan serangan Salt and Pepper Noise dan memastikan keutuhan data selama pengiriman melalui Google Drive. Secara keseluruhan, steganografi LSB terbukti menjadi solusi yang efektif dan efisien untuk keamanan data di PT Capture It. Berdasarkan kesimpulan yang sudah dijelaskan, penulis menyampaikan saran sebagai berikut: Pengembangan Alat Deteksi yang Lebih Baik: Selain mengembangkan metode penyisipan yang lebih canggih, penelitian juga perlu fokus pada pengembangan alat deteksi steganografi yang lebih baik. Ini akan membantu dalam menguji ketahanan metode steganografi yang digunakan dan memastikan bahwa metode tersebut tetap aman di masa mendatang; Integrasi dengan Metode Keamanan Lainnya: Menggabungkan steganografi dengan metode keamanan lain seperti enkripsi dapat meningkatkan keamanan data secara signifikan. Penelitian lebih lanjut dapat menjelajahi integrasi ini untuk memberikan solusi keamanan yang lebih komprehensif; dan Penggunaan Teknik Steganografi yang Lebih Kompleks: Meskipun metode LSB efektif, penelitian lebih lanjut dapat dilakukan dengan menggunakan teknik steganografi yang lebih kompleks untuk meningkatkan keamanan data. Teknik-teknik ini mungkin dapat menawarkan perlindungan yang lebih kuat terhadap upaya deteksi oleh alat-alat steganalisis yang lebih canggih.

DAFTAR PUSTAKA

[1] A. Khurana, and B. M. Mehta, "Comparison of LSB and MSB based Image Steganography," *International Journal of Computer Science And Technology*, vol. 3, no. 3, pp. 870-871, 2012.
[2] D. R. I. M. Setiadi, et al, "Teknik Penyembunyian dan Enkripsi Pesan pada Citra Digital dengan Kombinasi Metode LSB dan RSA", *Jurnal Teknologi dan Sistem Komputer*, vol. 6, no. 1, pp. 37-43, 2018.
[3] C. Jatmiko, et al, "Uji Performa Penyisipan Pesan Dengan Metode LSB Dan MSB Pada Citra Digital Untuk Keamanan Komunikasi", *Dinamika Rekayasa*, vol. 14, no. 1, pp. 47-45, 2018.
[4] S. W. N. P. S. Mendrofa, A. Azannudin, V. W. Sari, "Implementasi Steganografi Dan Kriptografi Data Pasien Pada Klinik Pratama Siti Rahmah Menggunakan Metode Least Significant Bit dan Algoritma RC4", *Jurnal CyberTech*, vol.2, no.4, pp. 1-15, 2019.
[5] B. J. Simbolon, "Steganografi Penyisipan Pesan Pada File Citra Menggunakan Metode LSB (Least Significant Bit)," *Jurnal Nasional Komputasi dan Teknologi Informasi*, vol. 4, no. 1, pp. 1-6, 2021.
[6] J. R. Maulidina, N. B. Idris, and D. Djumhadi, "Implementasi Steganografi dan Steganalisis Menggunakan Metode LSB (Least Significant Bit) Pada File Gambar", *Forbis: Journal Forensic Business Information Systems*, vol. 1, no. 1, pp. 14-19, 2024. Available online: https://journal.universitasmulia.ac.id/index.php/forbis
[7] U. Sara, M. Akter, and M. S. Uddin, "Image Quality Assessment through FSIM, SSIM, MSE and PSNR-A Comparative Study," *Journal of Computer and Communications*, vol. 7, no. 3, pp. 8-18, 2019. https://doi.org/10.4236/jcc.2019.73002
[8] A. Makandar, S. Kaman, R. Biradar, and S. B. Javeriya. " Impact of Edge Detection Algorithms on Different Types of Images using PSNR and MSE," *LC International Journal of STEM*, vol. 3, no. 4, pp. 1–11, 2023. https://doi.org/10.5281/zenodo.7607059
[9] D. Y. Prayuda, "Analisa Pengujian Kualitas Citra Steganografi Dengan Pendekatan Parameter PSNR dan MSE," *Prosiding SNASTIKOM: Seminar Nasional Teknologi Informasi & Komunikasi ke-* 8, 2021, pp. 233-241.
[10] M. R. Rambe, E. V. Haryanto, and A. Setiawan, "Aplikasi Pengamanan Data dan Disisipkan Pada Gambar dengan Algoritma RSA dan Modified LSB Berbasis Android", Konferensi Nasional Sistem Informasi (KNSI) 2018, pp. 724-729, 2018.